This record is a partial extract of the original cable. The full text of the original cable is not available.

CONFIDENTIAL SECTION 01 OF 05 OTTAWA 003169

SIPDIS

STATE FOR WHA/CAN-BREESE AND HOLT
STATE PASS FCC
DHS FOR FEMA, CBP, S&T DIRECTORATE (DOCKERY), INTERNATIONAL AFFAIRS (OPTICAN), IAIS AND EP&R
USDOC FOR 4320/OFFICE OF NAFTA/GWORD/TFOX; 3134/OIO/WESTERN HEMISPHERE

E.O. 12958: DECL: 10/21/2010
TAGS: EIND PTER ECON CA SPP
SUBJECT: CRITICAL INFRASTRUCTURE PROTECTION IN TELECOMS

REF: A. (A) 04 OTTAWA 1424 (OIL AND GAS PIPELINES)
¶B. (B) 04 OTTAWA 924 (VOICE OVER INTERNET PROTOCOL)
¶C. (C) 03 OTTAWA 2558 (ELECTRIC POWER)

Classified By: Economic Minister Counselor Brian Mohler
Reasons 1.4(d) and (g)

SUMMARY

¶1. (U) This message summarizes key views of Canadian players on the challenges of critical infrastructure protection in North America's telecom sector. It is based on a series of interviews held by Mission staff in September-October 2005 in Ottawa and Toronto with government and industry representatives.

¶2. (C) North America's existing telecom networks seem resistant to widespread failures, but there is room for further testing/analysis in this area. Expected rapid adoption of voice over internet protocol (VOIP) in the next few years could dramatically increase the vulnerability of our voice communications to large disruptions. The most serious threat may be Internet-borne software viruses. While certain regulatory measures could control this vulnerability, the GOC has been slow to take such steps and has not allocated substantial resources to this area. An additional major problem - as we encountered in other Canadian industries (refs A, C) - is that private firms are not willing to share key security information with GOC departments/agencies. END SUMMARY/INTRODUCTION.

OVERVIEW

¶3. (SBU) The United States and Canada have always closely integrated their public telephone systems. Where the systems meet, eight "primary gateways" govern traffic between the two countries. With few exceptions, calling to and from Canada is like calling long distance within the United States, and the technologies and standards are identical. Indeed, many key telecom products and services originated with Canadian players (e.g. firms such as Nortel, Mitel, Newbridge, and Research in Motion). The U.S. FCC cooperates closely with the Canadian Radio-Television and Telecommunications Commission (CRTC) and Industry Canada (IC).

¶4. (C) Some of our conclusions about critical infrastructure protection in this sector are similar to those we reached in studying the energy sector (refs A and C):

-- Natural disasters - particularly storms - have historically been the most familiar problem. In telecoms, prolonged power outages (of any origin) that might result from such disasters are a top concern.

-- The industry's big players have sophisticated systems to maintain reliable service, and they appear to understand their security challenges well.

-- On the security side, these players' relationships with government appear to be problematic. Governments have so far brought little to these relationships in terms of expertise, data, or resources.

LANDLINE PHONE SERVICE

¶5. (SBU) North America's conventional hard-wired telephone system (the "public switched telephone network" - PSTN) has evolved a robust network and claims 99.999 percent "availability." Industry experts attribute this reliability to several factors, some of which do not prevail in mobile communications, including:

-- The 100-plus-year evolution of the industry.

-- A small number of industry players.

-- Competent regulation in the public interest.

¶6. (C) Industry security experts admit that there may be considerable room for improvement in PSTN reliability. Their suggestions include:

-- Longer backup power. PSTN facilities typically have backup batteries and generators with at most 8 to 24 hours' worth of fuel on site. In the event of a long power outage over a wide area, they will have difficulty maintaining fuel supplies. The logical response would be storing more fuel and/or ensuring that these facilities have priority access to fuel during a blackout. (Comment: Such "priority service arrangements" during a crisis are no small matter, since they require someone to make judgments about "priority" and then enforce non-market supply arrangements over large sectors of the economy for unknown time durations. With hospitals, police and other emergency services competing for priority status for fuel, phone company representatives admitted to us that they sometimes have difficulty obtaining priority status. End comment).

-- An additional, growing problem is that landline phone bases with cordless handsets - now standard in homes - depend on house current and are not usable at all during an outage. Households will want at least one old-fashioned cord phone in these situations.

-- More security testing. Telecom industry experts admit that they focus their reliability efforts "in areas that customers will notice or care about." This means that resources are concentrated in areas such as customer data protection, and may be under-allocated to "insidious" risks that are improbable or that have not yet led to customer-noticeable effects. In this vein, one expert suggested that the PSTN's separate signaling traffic is under-protected relative to voice traffic, making signaling traffic the "weakest link." Another commented that the vulnerability of modern software switching systems to deliberate hacking is unknown, since the industry has made no systematic effort to test their resistance. (Comment: A cybersecurity consultant claimed that hacking of software switches was his primary concern for the reliability of PSTNs. End comment.)

MOBILE PHONES

¶7. (SBU) A variety of mobile communications technologies are on the market, one of the most innovative (and in some ways the most secure and reliable) being the Canadian-developed "BlackBerry" messaging device. Because most mobile systems are served by towers spaced a few miles apart, many towers would have to fail simultaneously in order to cause a service outage over a wide area. While the mix of mobile technologies provides lower and spottier reliability than the PSTN, it also provides a degree of redundancy, making a complete failure of mobile communications unlikely in a diversified market.

¶8. (C) Industry experts admit to a range of vulnerabilities in mobile networks. All of these vulnerabilities become more serious as North Americans become more reliant on mobile phones. The problems include:

-- Backup power. Cellphones need recharging on a daily basis, so they will die off during a long power outage. Also, each tower needs to be provided with a battery, generator and fuel tank in order to operate during a blackout. Not only is this difficult in some cases (e.g. many cell towers are on rooftops), but the problem of maintaining access to fuel during a long blackout is much more complex than with the landline network.

-- Local overload. If too many mobile users crowd into a small area during an emergency, the network can become overloaded and fail just when and where it is most needed. (This problem is worsened by "BlackBerry" and similar devices, which are always connected to the network even when not in use. Comment: one phone company executive described a scenario where, after a power outage, all Blackberry units in an area simultaneously attempt to gain access at once, triggering a denial-of-service response from the network which can be mistaken for a deliberate attack. End comment.) Preventing this "overload" problem could require firms to over-invest in capacity throughout their networks, raising their costs significantly. Another approach is to create "priority service lists" of numbers which receive service first from an overloaded network. (Comment: Industry Canada officials described evolving plans for a priority service list for mobile phones that would, in the event of an emergency, cut off service to anyone not on the priority service list. This all-or-nothing approach was not what mobile-phone company executives had described to us; they had suggested a system of prioritizing users. End comment.)

-- Radio jamming. Suitcase-sized "jammers" (which generate white-noise radio signals) can block all cellphone transmissions (including those to "priority service lists") over a limited area. While it would take dozens to hundreds of these devices to block service across a major city, larger jammers can conceivably be built or bought from military sources. (Comment: while stating that these jammers are illegal in Canada, more than one industry interlocutor made oblique references to President Bush's 2004 visit, in which they suggested that their systems had been affected by jammers used in conjunction with the visit. End comment.)

-- Major switching offices (MSO's). Each of these supports one company's mobile network over a large region (e.g. one major firm has two MSO's serving Ontario's market area of ten million people). Overlapping disasters/attacks at several MSO's could conceivably interrupt service for a sustained period over such a region.

VOICE OVER INTERNET PROTOCOL (VOIP)

¶9. (C) Voice communications through the Internet are increasingly available and this technology may be adopted widely over the next two to three years - especially for internal communications within organizations -- because it allows voice service to be offered for a fraction of the cost of existing technologies. Industry security experts stressed to us that currently, regulators cannot even track which firms are offering VOIP ("any crook can get into the business"). They expressed concern that rapid uptake of VOIP could dramatically increase the vulnerability of North America's communications, unless VOIP's currently high exposure to power outages, viruses and other risks is mitigated.

¶10. (C) In both the United States and Canada, there are ongoing controversies at the regulatory level about whether and how VOIP services should be regulated. The Canadian regulator, the CRTC, has expressed the view that VOIP is functionally the same as conventional telephony and that a similar regulatory regime should apply (ref B), but Bell Canada and Internet service providers dispute this, and the CRTC is reportedly showing little movement toward effective regulation. At any rate, such regulations as are applied may be aimed less at network protection than at other goals (such as competition policy, and ensuring support of 911 and other public services). One regulatory difficulty inherent in the VOIP design is the portability of numbers and the inability to obtain a physical location for a VOIP call: this is an obvious problem for providing 911 emergency services, but also raises fraud and security issues.

¶11. (SBU) Our interlocutors offered the following general points of advice (some of which may well be self-interested) on how to make VOIP less vulnerable:

-- Limit the number of players, even if only because regulators only know how to achieve regulatory goals through a finite number of firms. This necessitates somehow restricting the offering of VOIP services to North Americans from offshore. (Comment: of all the suggestions, this seemed to be the most self-interested. End comment.)

-- Require VOIP phones to switch automatically to landline telephone power whenever their own power fails.

-- Respect principles developed over the decades in the PSTN. One such rule states that any call which begins and terminates in Canada (or the USA) should be routed in-country. Another is an engineering maxim for preventing failure: "Keep all the smarts in the network and make the terminals dumb."

ROLE OF GOVERNMENT

¶12. (SBU) Telecommunications are under federal government jurisdiction in Canada. The GOC has a recently amalgamated department - Public Safety and Emergency Preparedness Canada or PSEPC - which is analogous to U.S. DHS. However, responsibility for critical infrastructure protection in telecoms is partly delegated to Industry Canada, which is also responsible for telecom regulation and radio frequency allocation, and thus is home to much of the GOC's civilian expertise on communications technology.

¶13. (C) Even more than in energy networks, we received the impression that security experts in the telecom industry attach little value to the GOC's role in critical infrastructure protection. The overwhelming fact is that the infrastructure is owned and understood only by the big utility companies. Even if government bodies allocate more resources to developing CIP expertise, they will remain outsiders. They thus have little bargaining power when trying to develop dialogues with the companies. Coercive approaches fail, since firms find ways to avoid disclosing anything in a form that government officials can use.

¶14. (C) Clearly, government funding in these areas is an ongoing constraint. One company official told us, "They (PSEPC) want our participation but they have no budgets which would allow them to share costs or develop joint programs." When emboffs asked Industry Canada what they thought the sector's vulnerabilities are, they replied that "a vulnerability assessment has been identified as a requirement" and would be addressed when funding is obtained. (Comment: While industry executives were relatively pragmatic in accepting how little value-added they perceive from the government, Industry Canada officials surprised emboffs with their level of self-confidence in this area. Industry Canada interlocutors repeatedly emphasized their close and productive ties to the telecom industry players and stated how grateful the industry was for their assistance. This disconnect is not an encouraging insight into Industry Canada's self-assessment capability. End comment.)

¶15. (C) A further problem affecting telecoms CIP is that firms have even less incentive than in the energy sector to share information with government players, given (1) the sensitivity of their proprietary technologies, and (2) the closeness between the Industry Canada offices responsible for CIP and those responsible for telecoms regulation. As one company official noted, the systems which are most vulnerable - mobile and VOIP - are also those where technology is evolving rapidly and competition is most intense. Another said plainly: "We don't want to admit our security problems to our regulators" - lest the companies become burdened with further regulatory requirements. In other words, until there is a visible boundary between government officials responsible for CIP and those responsible for regulating the telecoms market, these firms have a strong disincentive to talk to government about security issues. Their position is that they will inform the GOC about their vulnerabilities at the time of a crisis (but not before), and only if protected by a signed non-disclosure agreement.

¶16. (C) Finally, such government information as might be valuable to telecom firms is generally not made available to them in a useful way. As in the energy sector, companies complain that blanket "security alerts" convey no actionable information. One company official said, "We get nearly nothing useful from PSEPC by regular channels. The time-critical stuff never gets around in time and it's always piecemeal. Any useful information we get comes through personal relationships." This official said that the best capabilities in the GOC were in the military and related agencies, such as the Communications Security Establishment (CSE), and that what is required includes:

-- GOC security clearances for key company officials.

-- Direct computer links from security agencies to the major telecom companies.

-- Substantial budgets (he suggested C$5-10 million) for joint operations and investigations "or else all we do is sit around and talk."

Visit Canada's Classified Web Site at
http://www.state.sgov.gov/p/wha/ottawa

WILKINS